Cleverbridge Technical and Organizational Measures

The technical and organizational measures (TOMs) provided below apply to all standard service offerings provided by the Cleverbridge Group. Evidence of the measures implemented and maintained by Cleverbridge may be presented in the form of up-to-date attestations, reports, or extracts from independent bodies upon request from the Client.

1) Payment Card Industry Data Security Standard (PCI DSS):
   a) Cleverbridge is PCI DSS certified and shall maintain such certification during the Term of this Agreement. Therefore, Cleverbridge:
      i) Masks credit card numbers or bank details when displayed.
      ii) Maintains individual user-IDs for data processing systems as well as secure passwords according to PCI DSS standard.
      iii) Keeps storage of cardholder data at a minimum so that cardholder data is only stored for as long as necessary.
      iv) Maintains an up-to-date list of devices with the information specified by PCI for the clear identification of the devices and has implemented the measures provided by PCI DSS for the protection of devices against manipulation and replacement.
      v) Encrypts:
         (1) hard disks of the workstations (i.e. notebooks, PCs) used by employees for data processing.
         (2) credit card data in storage environment while at rest.
         (3) transmission of personal data from the credit card processor via public networks.
         (4) emails as needed or requested.
      vi) utilizes procedures for data backups according to PCI DSS standard.

2) Physical Security and Equipment Protection:
   a) All databases of the payment area are located on the servers in Cleverbridge's data center in a completely encrypted area.
   b) All servers used are located in an appropriately air-conditioned environment.
   c) Cleverbridge has installed appropriate fire protection measures in all areas where data processing takes place.
   d) Cleverbridge has implemented adequate power supply for systems by means of uninterruptible power supply (UPS).
   e) Physical security implemented on Cleverbridge premises includes:
      i) Badge-controlled access to buildings and secure areas where Cleverbridge IT networks are installed in such areas, with controlled access systems to limit access to restricted access areas to authorised personnel only.
      ii) Visitors allowed access to premises only when escorted by an authorised person with a record in the visitors register.
      iii) Security guard force present in certain selected buildings. CCTV in buildings.
      iv) Emergency response procedures in place for buildings in the case of fire, flood etc.

3) Security Incident Response/Prevention:
   a) Cleverbridge maintains an Incident Response Plan and a risk management process.
   b) Cleverbridge conducts regular vulnerability scans and penetration tests as well as use of intrusion detection and intrusion prevention systems.
   c) Cleverbridge equips all workstations and servers with anti-virus software that is updated automatically on a regular basis.
   d) Cleverbridge identifies security risks and all system components and regularly protects software applications with the latest security patches against known security risks to close security gaps.

e) Cleverbridge specifies criteria for secure development of applications developed in-house. After development, Cleverbridge checks the individual program code for all potential security risks (dual control principle) and makes corrections, if necessary.
f) To minimize the damage from security incidents:
    i) All incidents are reported through appropriate management and security incident reporting channels as quickly as possible.
    ii) All employees and contractors are made aware of the procedures for reporting the different types of security incident that might have an impact on classified information or on the information technology infrastructure and services.
    iii) Any physical security incidents, including security breaches or thefts, are reported immediately to the organization responsible for physical security.

4) Data Retention:
a) Cleverbridge has implemented policies and procedures for data retention and deletion (deletion periods and processes for deleting data). As soon as personal data, in whatever form (especially in paper or electronic form), is no longer required, Cleverbridge destroys personal data in a manner that makes recovery impossible.

5) User Access Management:
a) Cleverbridge has implemented:
    i) A roles and access rights concept.
        (1) Access authorizations are limited to the extent necessary to perform the activity according to responsibilities and information requirements (assignment of minimum authorizations according to the need-to-know principle).
    ii) Logging and protocol evaluation systems.
    iii) Strong cryptography and security protocols.
        (1) Only trustworthy keys and certificates are accepted. The protocol used supports only secure versions or configurations and the correct encryption strength is used.
    iv) Procedures to protect cryptographic keys against disclosure or misuse.
        (1) Key management processes and procedures for cryptographic keys are certified.
    v) Access controls and alarm systems for headquarters, video surveillance in server rooms as well as data centers.
    vi) A firewall configuration, or a demilitarized zone.
        (1) The firewall configuration is set up according to a standard defined for this purpose, is maintained regularly, and restricts incoming and outgoing connections between the internal company network and other networks.
    vii) A web application firewall to detect and prevent web-based attacks.
    viii) Separate development and test environments from the production environment.
    ix) Audit trails to track the entire access of individual users to system components or user activities in order to prevent or detect access protection violations and to identify the causes of problems.
    x) Systems to detect unauthorized changes (including additions and deletions) to critical system, configuration or content files.
b) All access to client facing environments require authentication through a secure connection via approved methods such as VPNs and enforced with mutual certificate authentication. VPN access is further enforced by mutual transport layer security authentication.
c) Cleverbridge controls internal and external distribution of any kind of media and classifies media for this purpose according to the risk potential of the contained data.
    i) Cleverbridge also maintains media inventory lists.

6) Additional commitments to Client:

a) Cleverbridge will maintain a record of all categories of processing activities carried out on Client's behalf to the extent required to enable Client to comply with its obligations under applicable data protection laws, and require any sub-processors to do the same.

b) Cleverbridge will also take reasonable steps to ensure the reliability and obligation to confidentiality of any person authorized to process personal data, and will implement and maintain appropriate technical and organizational data protection and security measures to ensure the security and accountability of the personal data as required under Article 32 of the GDPR and various provisions of the CCPA.

c) Cleverbridge will maintain policies and procedures that determine whether personnel and third parties engaged by Cleverbridge are suitable for their roles, and provide appropriate training and information. Cleverbridge maintains a security awareness program for personnel which provides training and awareness on corporate security policies and compliance with PCI-DSS

d) Cleverbridge will maintain business continuity and disaster recovery plans designed to maintain Cleverbridge's delivery of the services with minimal interruption. Each plan will detail measures to support the restoration of full operations as soon as possible after an emergency. The plans will addresses the need for failover capability and provision of an alternate recovery site based upon the criticality of the business functions, with input from the business owners. Plans will be periodically tested to make Cleverbridge's most critical business applications readily available in the event of a declared disaster. Backups will be stored offsite from the primary data source to support the recoverability of data importer systems in the event of a disaster.